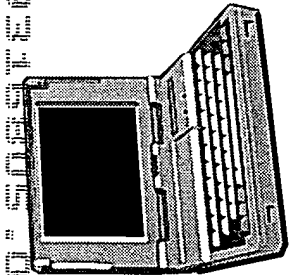


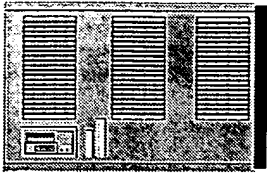
Fig. 1A



1003



1001



1005

1080 Send Cert. & Keys, Disconnect

Store Signed Certificate  
and Public Key 1085

Store Private Key 1090  
as Protected Value

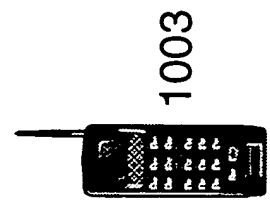
Delete PIN

1095

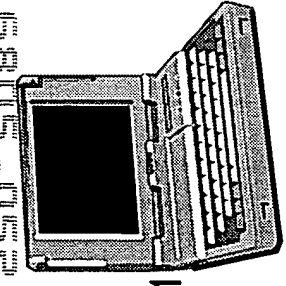
Delete PIN

Fig. 1B

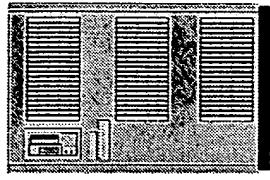
5 1 2 3 4 5 6 7 8 9 1 0 1 1 1 2 1 3 1 4 1 5 1 6 1 7 1 8 1 9 2 0



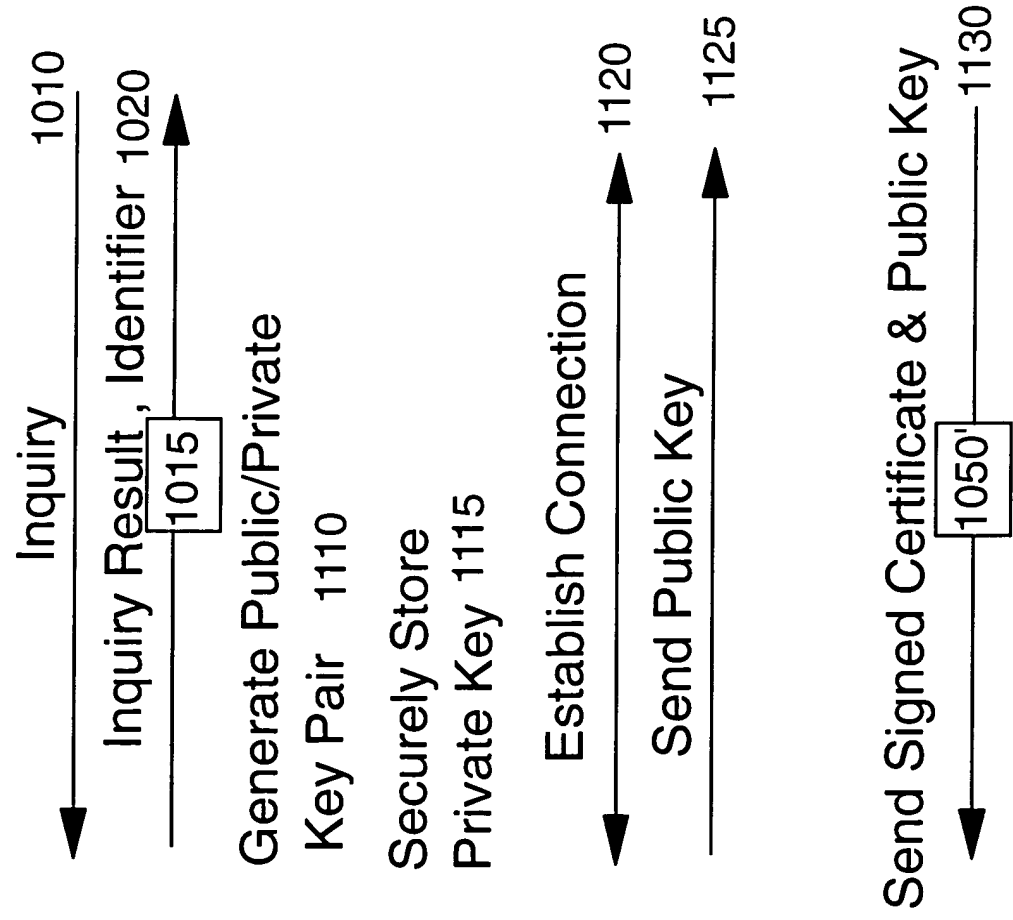
1003



1001

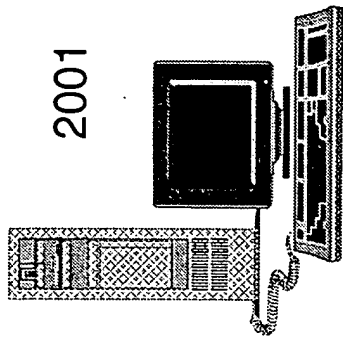


1005



Same as Steps in  
Figure 1A & 1B

Fig. 1C



2001



2003

# Authentication

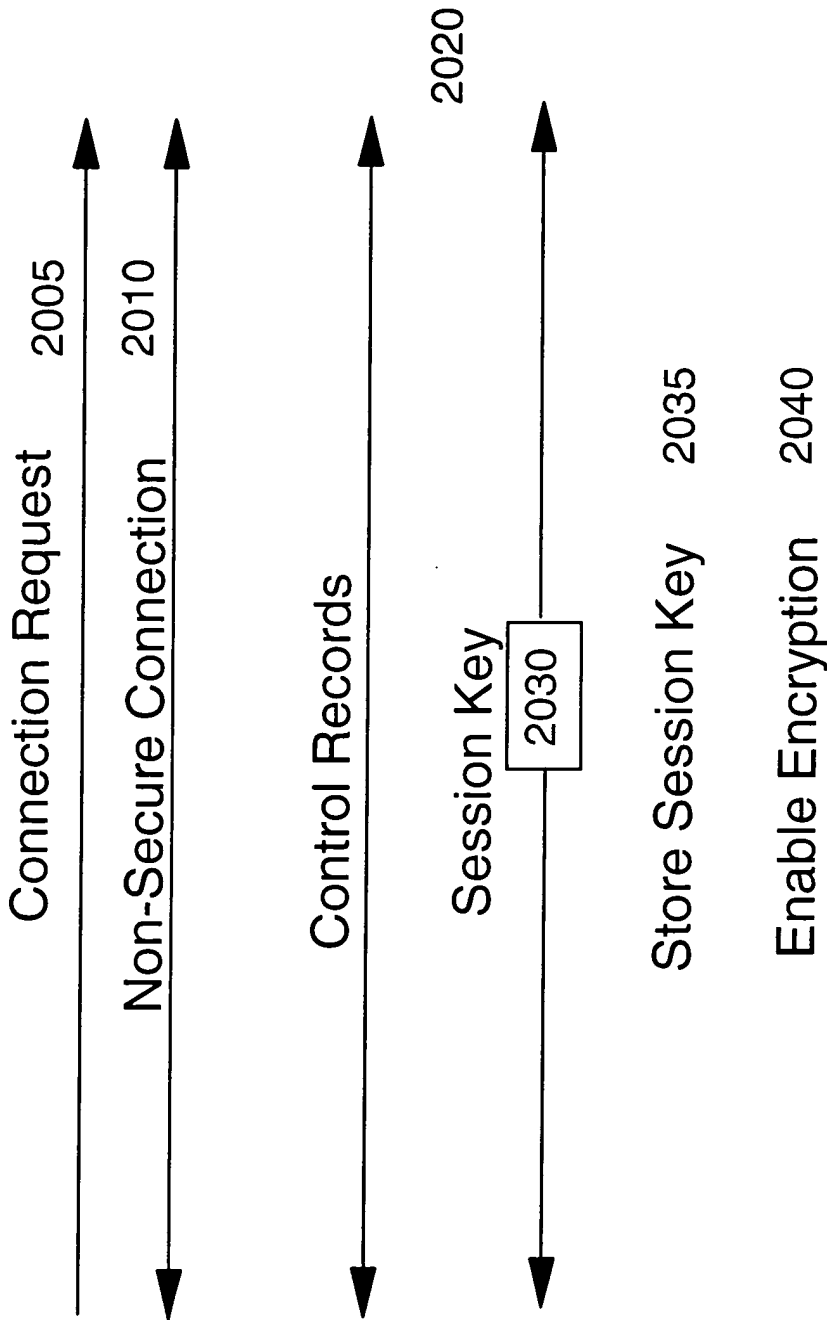


Fig. 2

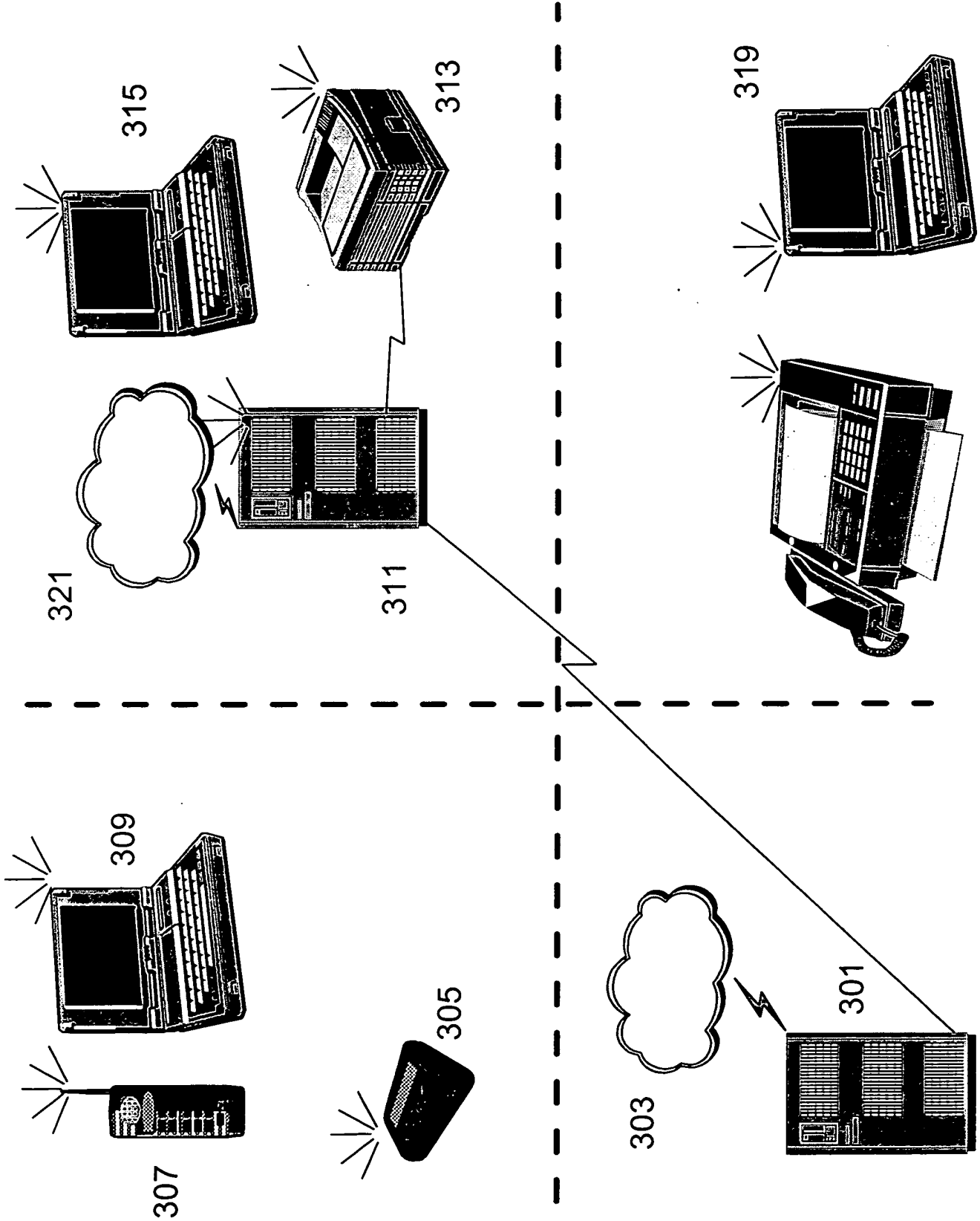
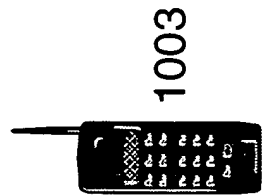


Fig. 3

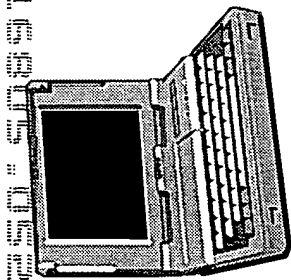
1050'

Device Identifier	4010
Public Key	4015
Optional Data	4020

Fig. 4

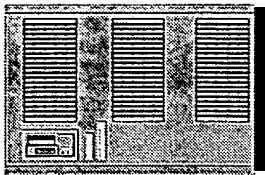


1003



5001

607-330-5050



1005

Authentication & Encryption 5010

Request Access 5020

Request Authorization 5030

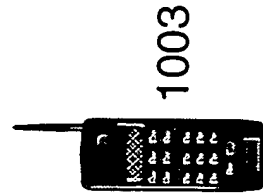
5040 Consult Database

Granted or Denied

Granted or Denied

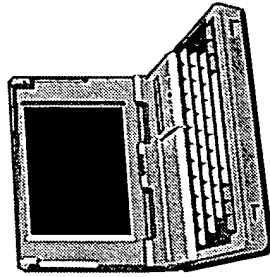
5050

Fig. 5A



1003

5001 5010 5020



5001

Authentication & Encryption

5010

Request Access

5020

Examine Optional  
Data in Certificate

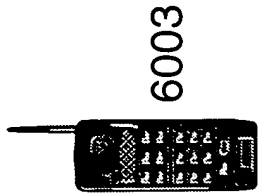
5100

5110 Determine Authorization

Granted or Denied

5150

Fig. 5B



Head Set 6001

6003

Unpaired 6010 Unpaired  
Device Certificate Present Device Certificate Present

User Initiates Pairing 6020 User Initiates Pairing

6030 Authentication Flows

6040 Display Device ID from Certificate

User compares device ID displayed with 6050  
externally provided device ID

User accepts pairing if they match 6060

User rejects pairing if they don't match 6070

Fig. 6